biprefix codeの1つの族について(代数的コード理論と関連分野)

AUTHOR(S):

中畑, 登

CITATION:

中畑, 登. biprefix codeの1つの族について(代数的コード理論と関連分野). 数理解析研究所講究録 1989, 697: 70-89

ISSUE DATE:

1989-06

URL:

http://hdl.handle.net/2433/101437

数理解析研究所講究録
697巻 1989年 70-89

biprefix codeの1つの族について

東海大学短期大学部　中畑　登　(Noboru Nakahata)

この論文ではbiprefix codeの1つの族を構成する。ただしこの族はかなり大きなもので、その一般的な構造は複雑である。そこでこの族の部分族として興味あると思われるものを中心に考察する。特に、この部分族に属するcodeのsyntactic monoidを完全に決定する。

1　基本的な用語と命題

Aをn個の元からなる有限集合とし、これをalphabetと呼ぶ。Aの各元を文字と呼び、文字の有限列を語という。文字を含まない語というものを考え、これを空語といって記号1で示す。語の全体をA^*で示す。uとvを任意の語とし、$u=a_1\cdots a_p$, $v=b_1\cdots b_q$ $(a_i, b_j\in A)$とするときuとvの積を、$uv=a_1\cdots a_p b_1\cdots b_q$で定める。空語1をこの演算の単位元と考えて$A^*$はmonoidの構造を持つ。このmonoidをA上のfree monoidと

いう。$w=u\cdot v$ $(u,v\in A^*)$ と置くとき、u を $(v$ を$)w$ の左(右)因子という。A^* の任意の部分集合を言語という。2つの言語 L、L' に対してその積を $L\cdot L'=\{l\cdot l' \mid l\in L,\ l'\in L'\}$ と定める。もし $L=L'$ のときは、$L\cdot L=L^2$ 等と巾の形で表す。$A^+=A^*\setminus\{1\}$ とおく。

定義1.1. M を A 上の言語で 1 を含むとする。もし $M=M^2$ が成り立つとき、M を A^* の submonoid という。

定義1.2. L を A 上の言語とする。空語 1 及び L の元の有限個の積全体を L^* で示す。L^* は明らかに A^* の submonoid である。これを L から生成された submonoid という。

定義1.3. M を A^* の submonoid とする。集合 $(M\setminus\{1\})\setminus(M\setminus\{1\})^2$ を M の base という。これを今 C で表すとき、$M=C^*$ が成り立つ。もし M が、$M=D^*$ と表されていれば、C は D に含まれていることが定義よりわかる。そこで C を M の minimal generator という。

定義1.4. C を A 上の言語とする。C の任意の元 $x_1,\cdots,x_p$, $y_1,\cdots,y_q$ に対して、もし $x_1\cdots x_p=y_1\cdots y_q \Rightarrow p=q$、$x_i=y_i$ $(i=1,\cdots,p)$ が成立するとき、C を A 上の code という。

定義1.5. A^*のsubmonoid Mが unitaryとは、任意の語wに対して もし $Mw \cap wM \cap M \neq \emptyset \Rightarrow w \in M$ が成立するときをいう。

命題1.1. A^*のsubmonoidが unitary $\Leftrightarrow$ Mの baseが code

定義1.6. PをA上の言語とし、$1 \notin P$とする。もし、$P \cap PA^+ = \emptyset$ ($P \cap A^+P = \emptyset$)なら、PをA上の prefix code (suffix code) という。prefix code (suffix code) は定義1.4の意味で実際に codeになっている。

定義1.7. A^*のsubmonoid Mが右unitary (左unitary)とは、任意の $w \in A^*$に対して、$Mw \cap M \neq \emptyset$ ($wM \cap M \neq \emptyset$) $\Rightarrow w \in M$ を満たすときをいう。もしMが右及び左unitaryのとき、Mを biunitaryと呼ぶ。

命題1.2. A^*のsubmonoid Mが右unitary (左unitary)
$\Leftrightarrow$ Mの baseが prefix code (suffix code)

biprefix codeの例として次のものがある:
ηをA^*から群Gの上への写像とする。又HをGの任意の部分群とする。このとき$\eta^{-1}(H)$はA^*のbiunitaryなsubmonoidになるこ

とが確かめられる。従ってその base は A 上の biprefix code になる。これを我々は group code と呼ぶ。

2. biprefix code の構成

この節の目的は biprefix code の1つの族を構成することである。$A=\{a_1, a_2, \cdots a_n\}$, $n \geqslant 2$ とする。G を任意の群とし、g_0 を G の1つの固定された元とする。又 $\Sigma=[\sigma_{ij}]$ を $n \times n$ 行列とし、各成分 σ_{ij} は G から G への1対1の準同型写像とする。Σ を指示行列と呼ぶ。σ_{ij} の G の元 g への作用は $g\sigma_{ij}$ と書くことにする。さて、A^* の元 w の各文字に G の元を次の方法で付けていく：

(1) g_0 は各文字 a_i に付ける。

(2) $w=a_i \cdot a_j \cdots a_k \cdot a_\ell \cdots a_m$ とする。このとき g_0 は w の最初の文字 a_i に付ける。そして $g_0\sigma_{ij}$ は g_j に付ける。もし $g_0\sigma$ が a_k に付いていたら、a_ℓ には $g\sigma_{k\ell}\sigma$ が付けられる。この様にして w のすべての文字に G の元が付けられる。

(3) G の単位元 1 は A^* の空語 1 に付く。

さて、A^+ の各元 w、各 $i=1, \cdots n$ に対して $\gamma_i(w)$ を、w の中の文字 a_i に付いている G の元の積とする。もし a_i が w の中に現われないときは $\gamma_i(w)=1$ とする。特に $\gamma_i(1)=1$ である。以上で A^*

の各元 w に対して1つの元 $(\gamma_1(w), \cdots, \gamma_n(w)) \in \overbrace{G \times \cdots \times G}^{n} = G^n$ が対応する。この写像を γ で表す。このとき次の命題が成り立つ。

命題2.1. 任意の $u, v \in A^*$ に対して、

$$\gamma(u \cdot v) = \gamma(u)(\gamma(v)\sigma)$$

が成り立つ。ここで σ は u と v に関係する G から G への1対1の準同型写像であり、$\gamma(v)\sigma = (\gamma_1(v)\sigma, \cdots, \gamma_n(v)\sigma)$ と定める。

さて $M = \{w \in A^* \mid \gamma(w) = (1, \cdots, 1)\}$ とおくとき、次が導かれる。

命題2.2. M は A^* の biunitary な submonoid である。

上で定義した M は、G^n の自明な部分群 $(1, \cdots, 1)$ の γ による逆像であるが、もう少し一般化して次の性質を持つ部分群を考える：　任意の $\sigma_{ij} \in \Sigma$ に対して、

(i) $H\sigma_{ij} \subset H$

(ii) $g\sigma_{ij} \in H \Rightarrow g \in H$

我々はこの様な H を Σ-不変な部分群と呼ぶ。このとき $M = \{w \in A^* \mid \gamma(w) \in H\}$ とおけば、やはり M は A^* の biunitary な submonoid になることがわかる。従ってその base は biprefix code になる。M の base を $\Gamma(H)$、M 自身を $\Gamma^*(H)$ で表すことにする。任

意に与えられた Σ, H に対して $\Gamma^*(H)$ 又は $\Gamma(H)$ を考察することは非常にむずかしい様に思われる。そこで次の特別な場合を選ぶことにする：

(1). G として整数の加法群 $\mathbb{Z}$、g_0 として 1 を考える。

(2). ε を $\mathbb{Z}$ の自明な自己同型写像、ε' を自明でない唯一の自己同型写像，即ち $k\cdot\varepsilon' = -k$, $k\in\mathbb{Z}$. 指示行列 $\Sigma=[\sigma_{ij}]$ として

(i). $\sigma_{ii} = \varepsilon$, $i=1,\cdots,n$

(iii). $i\neq j$ に対して、$\sigma_{ij}=\varepsilon$ 又は ε' であり、もし $\sigma_{ij}=\varepsilon$ ならば $\sigma_{ji}=\varepsilon'$ となる様に定める。$\Pi=\{(i,j)\mid \sigma_{ij}=\varepsilon\}$ とおく。

(3). H として、$\mathbb{Z}^n$ の任意の部分群を考える。明らかに H は Σ-不変である。

注意. $\mathbb{Z}^n$ は abel 群だから、加法の記号を採用する。$\mathbb{Z}^n$ の零元は単に 0 で示す。又 ε、ε' をそれぞれ 1、-1 で表すことにする。

例 2.1. $A=\{a,b\}$、ただし $a=a_1$、$b=a_2$. 指示行列 Σ を、

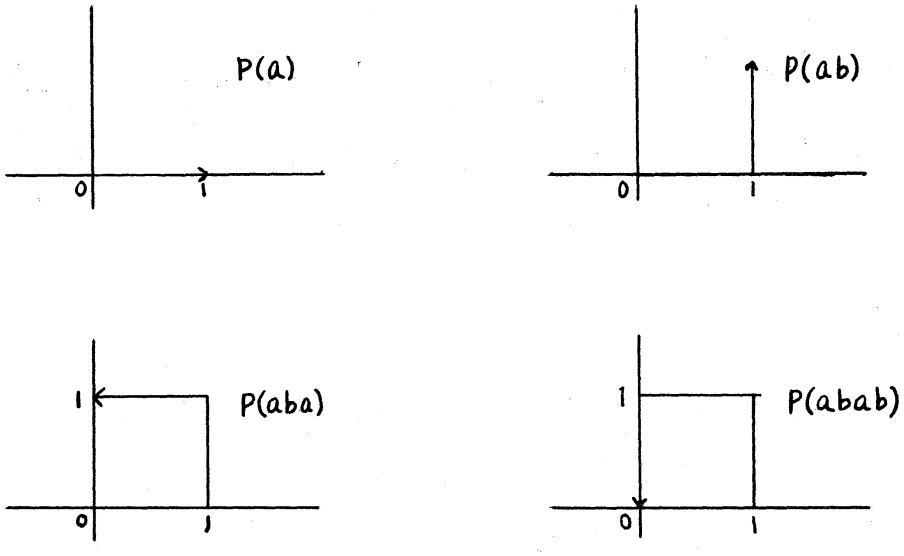
$$\Sigma=\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$$ とし、Σ-不変な部分群を $H=\{0\}$ とする。

w の各文字に付けられる 1 又は -1 を、その文字の下に書くこ

とにする。いくつかの語wに対して$\gamma(w)$を計算すると次の様になる。

1. $w=a$ このとき $w=\underset{1}{a}$ となり、$\gamma(a)=(1,0)$
2. $w=ab$ このとき $w=\underset{1\ 1}{ab}$ となり、$\gamma(ab)=(1,1)$
3. $w=aba$ このとき $w=\underset{1\ 1\ -1}{aba}$ となり、$\gamma(aba)=(0,1)$
4. $w=abab$ このとき $w=\underset{1\ 1\ -1\ -1}{abab}$ となり、$\gamma(abab)=(0,0)$

A^*の各元wに対して、1つの道$p(w)$をn次元の空間に対応させることができる。それは原点から出発して途中、点$\gamma(u)$を通り、終点$\gamma(w)$に終る道である。ただしuはwの各左因子である。$n=2$のとき、上の4つの語の道を次に示す:



語wが$\Gamma^*(\{0\})$に属することは、道$p(w)$が原点で終ることである。さて、仮定(1)(2)(3)のもとで$\Gamma^*(H)$の構造について考えて

いく。

定義 2.1. A上の言語Lに対して、$wA^* \cap L \neq \emptyset$ ($A^*w \cap L \neq \emptyset$) が任意の $w \in A^*$ に対して成り立つときLを右dense (左dense) という。

命題 2.3. $\Gamma^*(H)$ は右及び左denseである。

証明 $\Gamma^*(H) \supset \Gamma^*(\{0\})$ より、$\Gamma^*(\{0\})$ について示せばよい。$w = a_i \cdots a_j$ とする。又 $\Gamma^*(\{0\}) = \Gamma^*$ とおく。

Case 1: $(i,j) \in \Pi$, $i \neq j$

もし $w = a_i \cdots \underset{1}{a_j}$ ならば $w \cdot w = a_i \cdots \underset{1}{a_j}\, \underset{-1}{a_i} \cdots \underset{-1}{a_j}$ より $\gamma(w \cdot w) = \gamma(w) - \gamma(w) = 0$ となり、$w^2 \in wA^* \cap \Gamma^*$、$w^2 \in A^*w \cap \Gamma^*$。もし $w = a_i \cdots \underset{-1}{a_j}$ ならば、$u = w a_i a_j = a_i \cdots \underset{-1}{a_j}\, \underset{1}{a_i}\, \underset{1}{a_j}$ 及び $v = a_i a_j w = a_i \underset{1}{a_j}\, \underset{-1}{a_i} \cdots \underset{+1}{a_j}$ となる。従って $\gamma(u^2) = 0$ 及び $\gamma(v^2) = 0$ となり、$u^2 \in wA^* \cap \Gamma^*$、$v^2 \in A^*w \cap \Gamma^*$ となる。

Case 2: $(j,i) \in \Pi$, $i \neq j$

このときもCase 1と同様に考えて、$wA^* \cap \Gamma^* \neq \emptyset$、$A^*w \cap \Gamma^* \neq \emptyset$ を得る。

Case 3: $i = j$

このときは $k \neq i$ なる k を取り、語 wa_k、$a_k w$ をCase 1又はCase 2に適用すればよい。

定義2.2. L を A 上の言語とする。L による A^* の syntactic congruence $\equiv$ を次の様に定める： $u, v \in A^*$ に対して、

$$u \equiv v \iff \left[\text{任意の } p, q \in A^* \text{に対して、} puq \in L \Leftrightarrow pvq \in L\right]$$

定義より $\equiv$ は A^* の同値関係となり、さらに A^* の congruence になる。つまり $u \equiv u'$、$v \equiv v' \Rightarrow u \cdot u' \equiv v \cdot v'$ が成り立つ。以後 $\Gamma^*(H)$ による A^* の syntactic congruence について考える。このとき次の2つの場合が生じる：

(A) $\mathbb{Z}^n/H$ の任意の元 t に対して、$t = -t$ が成立する場合、つまり $\mathbb{Z}^n/H$ が位数が2のべきの基本abel群のとき。

(B) そうでないとき、つまり $t \neq -t$ となる $t \in \mathbb{Z}^n/H$ があるとき。

最初に(B)をあつかう。$\bar{\gamma}(w)$ を、$\gamma(w)$ の H を法とした剰余類とする。仮定(B)のもとで、$\equiv$ が次の様に特徴づけられる。

定理2.4. $w = a_i u \underset{r}{a_j}$、$w' = a_k u' \underset{s}{a_\ell}$ とする。このとき

$$w \equiv w' \iff \begin{cases} \text{(i)} & \bar{\gamma}(w) = \bar{\gamma}(w') \\ \text{(ii)} & a_i = a_k \\ \text{(iii)} & a_j = a_\ell \\ \text{(iv)} & r = s \end{cases}$$

証明. (i).(ii).(iii).(iv) が成立すると仮定する。$p, q \in A^*$ に対して $pwq \in \Gamma^*(H)$ のとき、$pw'q \in \Gamma^*(H)$ を示す。従って

$$\bar{0} = \bar{\gamma}(pwq) = \bar{\gamma}(pa_i u a_j q) = \bar{\gamma}(p) + x\{\bar{\gamma}(a_i u a_j) + y\,\bar{\gamma}(q)\} \qquad (1)$$

ここで、x は 1 又は -1 で p と a_i、そして p の最後の文字と a_i に付けられた値にだけ関係する。又 y については q と a_j、そして q の最初の文字と a_j に付けられた値にだけ関係する。(i)-(iii) より (1) 式は

$$\bar{0} = \bar{\gamma}(p) + x\{\bar{\gamma}(a_i u' a_j) + y\,\bar{\gamma}(q)\} \qquad (2)$$

となる。さらに (iv) より (2) の右辺は、まさに $\bar{\gamma}(pw'q)$ である。従って $pw'q \in \Gamma^*(H)$ となる。

逆に $w \equiv w'$ とする。(i) を示すため、最初から $a_i = a_k$ と仮定してよい。なぜなら、もし $a_i \neq a_k$ で仮りに $(i,k) \in \Pi$ であったとする。従って $\bar{\gamma}(a_i w) = \bar{\gamma}(a_i) + \bar{\gamma}(w)$, $\bar{\gamma}(a_i w') = \bar{\gamma}(a_i) + \bar{\gamma}(w')$ となる。又 $w \equiv w'$ より $a_i w \equiv a_i w'$ である。そこで、もし $\bar{\gamma}(a_i w) = \bar{\gamma}(a_i w')$ なら、$\bar{\gamma}(w) = \bar{\gamma}(w')$ がわかる。同じ理由で $a_j = a_l$ とする。

Case 1: $(i,j) \in \Pi$, $i \neq j$

(a) $w = a_i u a_j$ 又は $w' = a_i u' a_j$ (前者を仮定する)

このとき $\bar{\gamma}(ww) = \bar{\gamma}(w) - \bar{\gamma}(w) = \bar{0}$ となるから $w \cdot w \in \Gamma^*(H)$。$w \equiv w'$ より $ww' \in \Gamma^*(H)$ となる。従って $\bar{0} = \bar{\gamma}(w \cdot w') = \bar{\gamma}(w) - \bar{\gamma}(w')$ より、$\bar{\gamma}(w) = \bar{\gamma}(w')$ を得る。

(b) $w = a_i u a_j^{-1}$ 及び $w' = a_i u' a_j^{-1}$

このとき、$wa_ia_j = a_iua_{-1}^{j}a_i a_j \equiv w'a_ia_j = a_iu'a_{-1}^{j}a_i a_j$ である。従って(a)より $\bar{\gamma}(wa_ia_j) = \bar{\gamma}(w'a_ia_j)$ となり、又 $\bar{\gamma}(wa_ia_j) = \bar{\gamma}(w) + \bar{\gamma}(a_ia_j)$ 及び $\bar{\gamma}(w'a_ia_j) = \bar{\gamma}(w') + \bar{\gamma}(a_ia_j)$ より $\bar{\gamma}(w) = \bar{\gamma}(w')$ を得る。

Case 2: $(j,i) \in \Pi$, $i \neq j$

(a) $w = a_iua_{-1}^{j}$ 又は $w' = a_iu'a_{-1}^{j}$

このとき Case 1 (a) と同様に求める結果を得る。この場合 $i=j$ でも正しい。

(b) $w = a_iua_{1}^{j}$ 及び $w' = a_iu'a_{1}^{j}$

このときは、$wa_ia_{-1}^{j} \equiv w'a_ia_{-1}^{j}$ となり (a) を使って主張を得る。

Case 3: $i = j$

(a) $w = a_iua_{-1}^{j}$ 又は $w' = a_iu'a_{-1}^{j}$

このときは、Case 2 (a) を使って $\bar{\gamma}(w) = \bar{\gamma}(w')$ を得る。

(b) $w = a_iua_{1}^{j}$ 及び $w' = a_iu'a_{1}^{j}$

このとき、$k \neq i$ となる番号を取り、語 wa_k, $w'a_k$ に Case 1 又は Case 2 を適用して $\bar{\gamma}(w) = \bar{\gamma}(w')$ を得る。

以上で (i) が示された。次に (ii) を示す。$a_i \neq a_k$ と仮定して矛盾を出す。さて任意の $z \in A^+$ に対して $\bar{\gamma}(z)$ は $\pm\bar{\gamma}(a_p)$, $p=1,\cdots,n$ の適当な和として書かれる。我々は今 (B) を仮定し、さらに $\bar{\gamma}$ は上への写像となることもわかるから、少なくとも1つの a_m に対して $2\bar{\gamma}(a_m) \neq \bar{0}$ が成り立つ。$i \neq k$ より $(i,k) \in \Pi$ としてよい。$w = a_iua_j$, $w' = a_ku'a_k$ であった。さらに $2\bar{\gamma}(a_iua_j) \neq \bar{0}$ とし

てよい。もしそうでなければ wa_m を考えればよい。さて $(i,k) \in \Pi$ で $i \neq k$ と仮定したから、$a_k a_i^{-1} u a_j \equiv a_k a_k^{-1} u' a_\ell$ である。従って、$\bar{\gamma}(a_k a_i u a_j) = \bar{\gamma}(a_k) - \bar{\gamma}(a_i u a_j) = \bar{\gamma}(a_k a_k u' a_\ell) = \bar{\gamma}(a_k) + \bar{\gamma}(a_k u' a_\ell)$。$\bar{\gamma}(a_i u a_j) = \bar{\gamma}(a_k u' a_\ell)$ より $2\bar{\gamma}(a_i u a_j) = 0$ を得て矛盾となる。

以上で(ii)が示された。次に(iii)を示す。今までのことから、$w = a_i u a_j$、$w' = a_i u' a_\ell$、$w \equiv w'$、$\bar{\gamma}(w) = \bar{\gamma}(w')$ となっている。前と同様に $2\bar{\gamma}(a_i u a_j) \neq \bar{0}$ とする。もしそうでないときは、$a_m \cdot w$ を考えればよい。さて $j \neq \ell$ と仮定し、$(j,\ell) \in \Pi$ とする。

Case 1: $a_i u a_j^{-1} \equiv a_i u' a_\ell^{-1}$

このとき $a_i u a_j^{-1} a_j \equiv a_i u' a_\ell^{-1} a_j$ となる。ある $z \in A^*$ をとり、$a_i u a_j^{-1} a_j z \in \Gamma^*(H)$、$a_i u' a_\ell^{-1} a_j z \in \Gamma^*(H)$ とできる。これから

$\bar{0} = \bar{\gamma}(a_i u a_j^{-1}) + \bar{\gamma}(a_j z)$、$\bar{0} = \bar{\gamma}(a_i u' a_\ell^{-1}) - \bar{\gamma}(a_j z)$ を得る。

$\bar{\gamma}(a_i u a_j^{-1}) = \bar{\gamma}(a_i u' a_\ell^{-1})$ より $2\bar{\gamma}(a_i u a_j^{-1}) = \bar{0}$ となってしまう。

Case 2: $a_i u a_j^{-1} \equiv a_i u' a_\ell$

このとき、$a_i u a_j^{-1} a_j^{-1} \equiv a_i u' a_\ell^{-1} a_j^{-1}$ となるから上と同様に考えて矛盾を得る。

Case 3: $a_i u a_j \equiv a_i u' a_\ell^{-1}$ 又は $a_i u a_j^{-1} \equiv a_i u' a_\ell$

前者のときは、$a_i u a_j a_\ell \equiv a_i u' a_\ell^{-1} a_\ell^{-1}$ となり、今までの方法で矛盾を得る。後者も同様。

従って(iii)が示された。最後に(iv)を示す。もし主張が zw と zw'

について正しければ，wとw'についても正しい。そこで再び$z\bar{\gamma}(a_i u a_j) \neq \bar{0}$と仮定する。$a_i u a_j \equiv a_i u' a_j$より$a_i u a_j a_j \equiv a_i u' a_j a_j$である。従って，もし$r \neq s$なら今までの方法から$z\bar{\gamma}(a_i u a_j) = \bar{0}$となってしまう。

以上で定理が示された。

注意　$w \equiv 1$なら$w = 1$である。なぜなら，もし$w = a_i z$，$z \in A^*$なら$a_i z a_j \equiv a_j$ $(j \neq i)$となり定理の(ii)に反する。

仮定(A)のもとで次を得る。

定理2.5.　任意の$w, w' \in A^*$に対して，

$$w \equiv w' \iff \bar{\gamma}(w) = \bar{\gamma}(w')$$

証明．仮定(A)のもとでは，任意の$u \in A^*$に対して$\bar{\gamma}(u) = -\bar{\gamma}(u)$である。つまり$\bar{\gamma}$は$A^*$から$\mathbb{Z}^n/H$の上への準同型写像である。このことから求める主張が導かれる。

3. $\Gamma^*(H)$のsyntactic monoidの構造

この節では$\Gamma^*(H)$のsyntactic monoidについて考える。次の定理は定理2.5の結果である。

定理3.1.　$M = \mathrm{Syn}(\Gamma^*(H))$とおく。仮定(A)のもとで，$M \cong \mathbb{Z}^n/H$．

次に仮定(B)のもとで考えていく。次の概念が半群論から必要になる。

定義3.1. Mを任意のmonoidとする。次の3つのM上の同値関係をそれぞれ、$\mathcal{R}$、$\mathcal{L}$、$\mathcal{H}$で表わす:

$$m \mathcal{R} n \iff mM = nM$$

$$m \mathcal{L} n \iff Mm = Mn$$

$$m \mathcal{H} n \iff mM = nM \text{ 及び } Mm = Mn$$

これらの関係は半群論において基本的な役割をする。

定理3.2. ηをA^*から$M = Syn(\Gamma^*(H))$への自然な写像とする。即ち、$w \in A^*$に対して$\eta(w)$はwを含む類である。このとき、

$$\eta(w) \mathcal{R} \eta(w') \iff w \text{ と } w' \text{が同じ文字から始まる。}$$

証明は定理2.4を用いて示されるが、省略する。$\mathcal{L}$関係についても次が成り立つ:

定理3.3. $\eta(w) \mathcal{L} \eta(w') \iff w$ と w'が同じ文字で終る。

上の2つの定理より次がわかる:

定理3.4. $\eta(w) \mathcal{N} \eta(w') \Leftrightarrow w$ と w' が同じ文字で始まり同じ文字で終る。

次に、Mの各 $\mathcal{N}$-class ($\mathcal{N}$-equivalent な類)の構造を決定する。$A_0=\{1\}$、$A_i=\{a_i\} \cup \{a_i w a_i \mid w \in A^*\}$、$A_{ij}=\{a_i u a_j \mid u \in A^*\}$ とおく。ただし $i,j=1,\cdots n$、$i \neq j$。さらに $\eta(A_0)=H_0$、$\eta(A_i)=H_i$ $\eta(A_{ij})=H_{ij}$ とおく。定理3.4より、H_0. H_i. H_{ij} はMの $\mathcal{N}$-class を作ることがわかる。又、各 $\mathcal{N}$-class は乗法で閉じていることがわかる。従って半群論の一般論から、それらは群をなす。

定義3.2. S を任意の半群とする。S の部分集合 $J \neq \emptyset$ が、$S \cdot J \cdot S \subset J$ を満足するとき、J を S の ideal という。S 自身は S の1つの ideal である。もし、S が S 以外に ideal を持たないとき、S は単純と呼ばれる。

さて、$S=\mathrm{Syn}(T^*(H)) \setminus \{1\}$ とおく。このとき S が単純になることが確かめられる。又一般論より、S の各 $\mathcal{N}$-class は互いに同型な群になることがわかる。そこで1つの $\mathcal{N}$-class、例えば H_1 について考えればよい。

定理3.5. F を Z''/H と同型な群、η を F の自己同型写像で、$x \in F$

に対して、$x^g = x^{-1}$ なるものとする。このとき、F の $\langle g \rangle$ による半直積が H_1 と同型になる：　$H_1 \cong \langle g \rangle * F$.

補題　任意の $w \in A^+$ に対して $\bar{\gamma}(w) = \bar{\gamma}(w')$ 又は $-\bar{\gamma}(w')$ 及び $w' = a_1 \cdots a_1$ となる $w' \in A^*$ がある。

証明　$w = a_k \cdots a_2$ とおく。又 $u = a_1 a_k a_1 a_k w a_2 a_1 a_2 a_1$ とおく。ここで、もし $k=1$ ($l=1$) なら u の最初の(最後の)4つの文字は現われないとする。このとき $\bar{\gamma}(w) = \pm \bar{\gamma}(u)$ がわかる。もし u の最後の文字に値1が付いていればが求める語である。そうでないときは文字 a_j, $j \neq 1$ を取り、語 $w' = a_1 a_j a_1 a_j a_j a_1 a_j a_1 \cdot u$ を考えると、この語 w' が求めるものになる。

定理3.5の証明　$\mathbb{Z}^n/H$ は巡回群の直和である：

$$\mathbb{Z}^n/H = \langle g_1 \rangle \oplus \cdots \oplus \langle g_l \rangle, \quad l \leq n.$$

補題より、必要なときは g_i を $-g_i$ にして、初めから $g_i = \bar{\gamma}(w_i)$, $w_i = a_1 u_i a_1$ としてよい。$\eta(w_i) = h_i$ 及び $\eta(w) = g$ とおく。ただし $w = a_1 a_s a_1$ $(s \neq 1)$。このとき g^2 は中等元になることがわかる。つまり H_1 の単位元である。$g^2 = e$ とおく。次に各 i に対して $g h_i g^{-1} h_i = e$ となる。実際、$u = a_1 a_s a_1 w_i a_1 a_s a_1 w_i$ とおくと定理2.4のすべての条件が、u と w^2 に対して成り立つ。従って、$u \equiv w^2$ となる。これは $\eta(u) = \eta(w)\eta(w_i)\eta(w)\eta(w_i) = \eta(w^2) = e$ を意味

する。つまり $g^{-1}h_i g h_i = e$ 又は $g^{-1}h_i g = h_i$ となる。

次に、F を $h_1, \cdots, h_\ell$ から生成された群とする。F が、巡回群 $\langle h_1 \rangle, \cdots \langle h_\ell \rangle$ の直積になることを示す。そのために、$h_1^{m_1} \cdots h_\ell^{m_\ell} = e$ と仮定する。これは A^* の中で考えると $w_1^{m_1} \cdots w_\ell^{m_\ell} \equiv w^2$ を意味し、従って $\overline{\gamma}(w_1^{m_1} \cdots w_\ell^{m_\ell}) = m_1 g_1 + \cdots + m_\ell g_\ell = \overline{\gamma}(w^2) = \overline{0}$ となる。従って $m_i g_i = \overline{0}$ となり、さらに $w_i^{m_i} \equiv w^2$ を得る。これは $\eta(w_i^{m_i}) = h_i^{m_i} = \eta(w^2) = e$ を意味する。即ち、F は $\langle h_1 \rangle, \cdots \langle h_\ell \rangle$ の直積である。最後に、H_1 は F と $\langle g \rangle$ によって生成されていることを示す。z を A_1 の任意の元とする。このとき、語 u を次の様に定める：

$$u = z \quad (z = a_1 \cdots \underset{1}{a_1} \text{ のとき}) \quad (1)$$

$$u = wz \quad (z = a_1 \cdots \underset{-1}{a_1} \text{ のとき}) \quad (2)$$

$\overline{\gamma}(u) = m_1 g_1 + \cdots + m_\ell g_\ell$ と表示する。このとき、u と、$v = w_1^{m_1} \cdots w_\ell^{m_\ell}$ は合同になる。従って $\eta(u) = \eta(v) = h_1^{m_1} \cdots h_\ell^{m_\ell}$ となる。これは、(1) 又は (2) に従って $\eta(z) = h_1^{m_1} \cdots h_\ell^{m_\ell}$ 又は $\eta(w)\eta(z) = h_1^{m_1} \cdots h_\ell^{m_\ell}$ を意味する。$\eta(w) = g = g^{-1}$ より、H_1 の任意の元 $\eta(z)$ は、群 $\langle g, F \rangle$ に属する。従って $H_1 = \langle g, F \rangle = \langle g \rangle * F$ となる。

群 H_1（S のすべての $\mathcal{H}$-class と同型になっている）を code $\Gamma(H)$ の群と呼ぶ。これについての詳しいことは [1] 又は [2] を参照。

4. いくつかのcodeの例とその群

この節では簡単なcodeの例を4つ与える。code $\Gamma(H)$ は $\mathbb{Z}^n$ の部分群Hによって定まる。$\mathbb{Z}^n$ は有限生成な自由abel群だからHが自明でなければ、Hは基 $w_1, \cdots, w_t$ を持つ。そこでcode $\Gamma(H)$ をこの基と同一視して、行列

$$\begin{bmatrix} w_1 \\ \vdots \\ w_t \end{bmatrix}$$

で表すことにする。前の様に $A=\{a, b\}$、$a=a_1$、$b=a_2$、

$$\Sigma = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$$

とする。又、C_m、D_m をそれぞれ位数mの巡回群、2面体群とする。

例4.1. $H=\mathbb{Z}(2,0)+\mathbb{Z}(0,1)$ このとき

$$\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} = \{b\} \cup \{ab^i a \mid i \geq 0\}$$ 図4.1.

Hの点から出発し、初めてHの点に終る道 $p(w)$ に対して、wがcode $\Gamma(H)$ の元となる。このcodeの群は、定理3.1より C_2 である。

例 4.2. $H = \mathbb{Z}(2,0) + \mathbb{Z}(1,1)$ のとき

$$\begin{bmatrix} 2 & 0 \\ 1 & 1 \end{bmatrix} = \{a^2, ab, ba, b^2\}$$ 図 4.2.

この code の群も C_2 である。

例 4.3. $H = \mathbb{Z}(3,0) + \mathbb{Z}(0,1)$ のとき

$$\begin{bmatrix} 3 & 0 \\ 0 & 1 \end{bmatrix} = \{b\} \cup \{ab^h a \mid h \geq 1\} \cup a^2 \cdot \{b^k a \mid k \geq 1\}^* a$$ 図 4.3

$\mathbb{Z}^2/H \cong C_3$ だから、定理 3.5 よりこの code の群は D_6 となる。

例 4.4 $H = \mathbb{Z}(3,0) + \mathbb{Z}(1,1)$ のとき

$$\begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix} = \{a^3, a^2ba, a^2b^2, ab, ba^2, (ba)^2, bab^2, b^2a, b^3\}$$ 図 4.4

$\mathbb{Z}^2/H \cong C_3$ より、code の群は D_6 である。

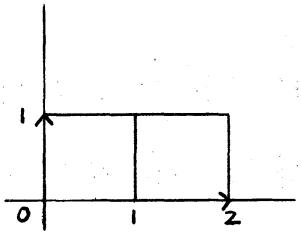


図 4.1

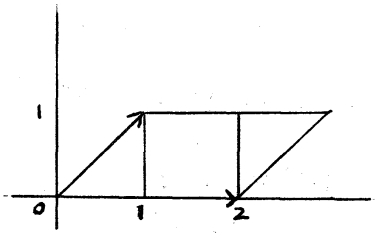


図 4.2

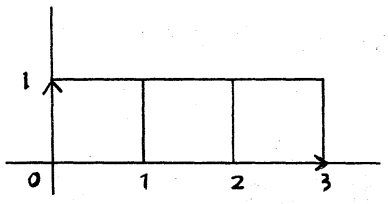


図4.3

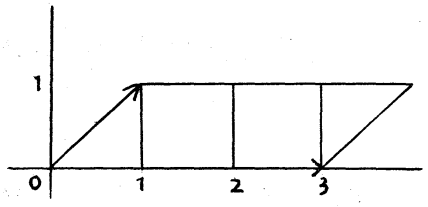


図4.4

命題4.1. $\mathbb{Z}^n/H$ が位数 d の有限群とする。このとき、各 $a_i \in A$ に対して、$a_i^{d_i} \in \Gamma(H)$ となる d の約数 d_i が一意的に定まる。

証明. 仮定より n 個のベクトル $u_1, \cdots, u_n$ があり H を生成する。そのとき、行列 $D = [{}^t u_1, \cdots {}^t u_n]$ は正則で、d は行列 D の行列式の絶対値に等しい。さらに各 $i = 1, \cdots, n$ に対して、$x_1 u_1 + \cdots + x_n u_n = (0, \cdots, \overset{i}{d}, \cdots, 0)$ となる整数 $x_1, \cdots, x_n$ が存在する。$\gamma(a_i^d) = (0, \cdots, \overset{i}{d}, \cdots 0) \in H$ より $a_i^d \in \Gamma^*(H)$ となり、$\Gamma(H)$ は code だから、求める d_i が存在する。

参考文献

[1]. Lallement, G. 1979. "Semigroups and Combinatorial Applications"

[2]. Berstel, J., Perrin, D. 1985. "Theory of Codes." Academic Press, London, New York.